REMARKS

Claims 1-67 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 103(a) Rejections:

The Examiner rejected claims 1, 4-10, 19, 21-26, 36, 38-42, 48, 52-60, 62, 66 and 67 under 35 U.S.C. § 103(a) as being unpatentable over Chen et al. (U.S. Patent 6,763,365) (hereinafter "Chen") in view of Bhushan et al. (U.S. Publication 2002/0174157) (hereinafter "Bhushan"), claims 2, 3, 15-18, 27-29, 35 and 43-46 as being unpatentable over Chen and Bhushan and further in view of Lasher et al. (U.S. Patent 4,863,247) (hereinafter "Lasher"), claims 11, 20, 30, 31, 37, 47 and 61 as being unpatentable over Chen and Bhushan and further in view of Stribaek et al. (U.S. Patent 7,181,484) (hereinafter "Stribaek"), and claims 12-14, 32-34, 49-51 and 63-65 as being unpatentable over Chen and Bhushan and further in view of Chen et al. (U.S. Patent 6,687,725) (hereinafter "Chen2"). Applicants respectfully traverse these rejections for at least the following reasons.

Regarding claim 1, contrary to the Examiner's assertion, the cited art fails to teach or suggest *a first arithmetic circuit comprising a first plurality of arithmetic structures feeding back high order bits of a previously executed arithmetic instruction in the public-key cryptography application, generated by the first arithmetic circuit, to a second arithmetic circuit comprising a second plurality of arithmetic structures*. The Examiner submits that these limitations are taught in Chen, col. 11, lines 34-40 (noting only, "feedback; first using circuit; then using circuit again with register provided with output from first operational stage"), and col. 10, lines 13-26 (noting only, "multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A, B"). However, the cited passages clearly do not teach or suggest the above-referenced limitations. For example, nothing in the cited passages describes a first circuit *feeding back high order bits of a previously*

executed arithmetic instruction to a second circuit, much less to a second circuit that is currently executing a different arithmetic instruction, as recited in a subsequent limitation of claim 1. Instead, the "multiplication with feedback" described therein appears to refer to feedback provided between operational stages of Chen's system while executing a single multiplication instruction. For example, the cited passage in col. 11 describes the multiplication operation "AB mod N." In Chen, a hardware circuit may execute this single multiplication operation in two phases. However, there is no feedback of a partial result from a previously executed single arithmetic instruction (i.e., a different instruction) described. The Examiner's citation in col. 10 describes the operation of Chen's hardware circuit in more detail, but also does not describe feedback of a partial result from a previously executed single arithmetic instruction, as required by Applicants' claim.

Further regarding claim 1, the cited art fails to teach or suggest *the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction in the public-key cryptography application, the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit; storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application.* The Examiner submits that this entire collection of limitations is taught in Chen, col. 4, lines 8-11 (noting only, "multiplication and addition are performed by large circuits"); in col. 10, lines 13-36 (without including any remarks regarding this passage); and in col. 11, lines 34-40 (noting only, "feedback; first using circuit; then using circuit again with register provided with output from first operational stage (multiplication with feedback)"). The Examiner's remarks (quoted above) refer only generally to features that the Examiner believes are taught by the cited passages of Chen without describing how the Examiner believes these passages (or elements described therein) teach or suggest each of the above-referenced limitations of claim 1. Thus, the Examiner has failed to fully and

clearly state his ground of rejection of claim 1 and has therefore failed to establish a *prima facie* case of obviousness given that the burden of proof falls on the Office. Since the features noted by the Examiner do not correspond to the language recited in the above-referenced claim limitations, it is not clear or how the cited passages teach the specific limitations of claim 1 as arranged in the claim. The statute clearly places the burden of proof on the Patent Office to prove a *prima facie* rejection. *In re Warner*, 154 USPQ 173, 177 (C.C.P.A. 1967), *cert. denied*, 389 U.S. 1057 (1968). The Examiner's vague assertions, which lack a clear mapping between the teachings of Chen and Applicants' claim, cannot be said to establish a *prima facie* case of obviousness, with or without the addition of the Bhushan reference.

In addition, the cited passages do not teach or suggest all of the above-referenced limitations. For example, these passage do not describe *the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction*, i.e., a different arithmetic instruction than the *previously executed arithmetic instruction* recited in claim 1. As noted above, Chen does not describe the execution of two different arithmetic instructions in the manner recited in Applicants' claim.

In the Office Action mailed December 11, 2008, the Examiner submits, "Bhushan discloses wherein a previously executed single arithmetic instruction. (see Bhushan paragraph [0116], lines 14-20; instruction requires an operand, a result from a previous instructions, the result may be bypassed under the direction of bypass routing control)". First, Applicants are unclear what point the Examiner is trying to make regarding "a previously executed single arithmetic instruction," since his remarks are directed only to this phrase. **In addition, Bhushan is directed to a method and apparatus for performing equality comparisons in redundant form arithmetic, and has absolutely nothing to do with the limitations recited in Applicants' claim.** More specifically, Bhushan is directed to a method for bypassing standard output routing from a functional unit. This bypass mechanism allows the result of an addition or subtraction instruction performed while in redundant form to be made available to a comparison instruction (comparing the result with 0 or another value) without converting the result of the

addition or subtraction out of redundant form and then back into redundant form for use as an operand of the comparison instruction. The cited passage in Bhushan describes this bypass mechanism.

Applicants assert that the bypass mechanism of Bhushan teaches nothing about the above-referenced limitations of Applicants' claim, or any limitations of Applicants' claim. For example, Bhushan describes nothing about *a first arithmetic circuit comprising a first plurality of arithmetic structures feeding back high order bits of a previously executed arithmetic instruction in the public-key cryptography application, generated by the first arithmetic circuit, to a second arithmetic circuit comprising a second plurality of arithmetic structures* or *the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction in the public-key cryptography application, the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit; storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application.* Instead, Bhushan describes that if the result of a single arithmetic instruction happens to be explicitly specified as an operand of a subsequent comparison operation, the entire result of the single arithmetic instruction may be passed to a functional unit that is to perform the subsequent comparison instruction without passing it through a redundant conversion unit and/or register file. Therefore, at most, Bhushan teaches a method for more efficiently passing the entire result of an arithmetic instruction to the input of a circuit for performing a subsequent non-arithmetic (comparison) instruction, in response to the result being explicitly coded as an operand for the comparison operation. This clearly does not teach or suggest the above-referenced limitations of Applicants' claim. In addition, Bhushan does not teach or suggest that this bypass mechanism can be used in any situation other than when an arithmetic instruction is followed by a comparison instruction in which the result of the arithmetic instruction is to be compared to zero or another value. Such a situation is clearly not analogous to that of the two

arithmetic circuits recited in Applicants' claim, or to the addition, multiplication, and feedback operations recited therein.

The cited art also fails to teach or suggest *the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit.* The Examiner's general reference to "multiplication with feedback" and a description of a hardware circuit usable to execute a single multiplication instruction (as in Chen), and to the bypass mechanism of Bhushan clearly do not teach these specific limitations of claim 1.

Applicants further assert that the cited art clearly does not teach or suggest *storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application.* The cited passages in Chen do not describe anything about storing a partial result, or using the stored partial result in a subsequent computation in a public-key cryptography application. Instead, they describe the execution of a single multiplication instruction. In addition, in the passages cited by the Examiner in Bhushan, the result of an addition or subtraction instruction that is to be used in a subsequent comparison instruction is explicitly not stored, due to the bypass mechanism described above. **Therefore, Bhushan actually teaches away from storing a result of one instruction for use in a subsequent computation.**

As discussed above, the descriptions of individual features listed by the Examiner do not teach the specific combination of limitations recited in claim 1, as arranged in the claim. The Examiner is clearly attempting a piecemeal reconstruction of Applicants' invention in hindsight without consider the claimed invention as a whole. Such reconstruction is improper. *See, e.g., Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985). For example, a general reference to "multiplication with feedback" and a description of a hardware circuit usable to execute a

single multiplication instruction clearly do not teach the specific limitations recited in claim 1 regarding *feeding back high order bits of a previously executed arithmetic instruction... to a second arithmetic circuit*, and *the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number.* In another example, the Examiner's statement that "multiplication and addition are performed by large circuits" teaches nothing about the limitations recited in claim 1. Furthermore, the addition of the Bhushan reference, which describes a mechanism to bypass a conversion operation used in completely non-analogous situations, teaches nothing about Applicants' claimed invention.

Finally, the Examiner has not stated a proper reason to combine the teachings of the cited art. The Examiner submits that it would have been obvious to one of ordinary skill in the art "to modify Chen for a previously executed single instruction to generate a result as taught by Bhushan... in order to provide an efficient method for an uncomplicated arithmetic circuit that is capable of adding or subtracting numbers in redundant from and comparing a result without requiring propagation of carry signals. (see Bhushan paragraph [0062], lines 1-5." **Applicants assert that this passage merely describes a benefit of using Bhushan's own methods for performing equality comparisons in redundant number form. It has absolutely nothing to do with a benefit that may be applicable in the system of Chen or with the above-referenced limitations of Applicants' claim, both of which are directed to instructions involving feedback during multiplication operations.** Therefore the rejection is improper. In addition, there is nothing in Bhushan or Chen that teaches or suggests that Bhushan's method could be combined with the system of Chen in a way that would result in Applicants' claimed invention, since neither reference teaches the above-referenced limitations of Applicants' claim. In fact, it is not clear that it is even possible to combine the teachings of Chen and Bhushan, as suggested by the Examiner, since they are directed to completely different problem spaces and corresponding solutions. Thus, one of ordinary skill would not have combined the teachings of Bhushan with the teachings of Chen in the manner proposed by the Examiner.

To establish a *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974), MPEP 2143.03. As discussed in detail above, neither of the cited references teaches or suggests the above-referenced limitations of Applicants' claim, whether taken alone or in combination, and the Examiner has failed to state a proper reason to combine the references in teaching Applicants' claimed invention. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

For at least the reasons above, the rejection of claim 1 is unsupported by the cited art and removal of the rejection thereof is respectfully requested.

Independent claims 38 and 66 include limitations similar to those recited in claim 1 and discussed above, and were rejected for similar reasons. Therefore, the arguments presented above apply with equal force to these claims, as well.

Independent claim 21 includes limitations similar to those recited in claim 1 and discussed above, and was rejected for reasons similar to those discussed above regarding claim 1. In fact, the Examiner includes several of the same citations and notes several of the same features of Chen and Bhushan in rejecting claim 21. Therefore, Applicants traverse the rejection of this claim for at least the reasons presented above regarding limitations in this claim that are similar to those in claim 1.

In addition, claim 21 recites *supplying a third number to the second arithmetic circuit* and *the first partial result being a representation of the high order bits summed with low order bits of a result of a first number multiplied by a second number and with the third number.* **The Examiner does not address this limitation.** Therefore, the Examiner has failed to state a *prima facie* rejection of claim 21. Applicants assert that the Examiner's citations and remarks regarding "multiplication and addition are performed by large circuits," "multiplication with feedback," "arithmetic operations to support acceleration of cryptographic functions", and the bypass mechanism of Bhushan

teach nothing clearly teach nothing about these limitations of claim 21. In addition, nothing in the cited passages describes a third number being supplied to any of the arithmetic circuits, much less one that is added to high order bits of a previously executed arithmetic instruction and low order bits of a result of a multiplication to produce a partial result, as in claim 21.

For at least the reasons above, the rejection of claim 21 is unsupported by the cited art and the removal thereof is respectfully requested.

Claims 53 and 67 include limitations similar to those recited in claims 1 and 21 and discussed above, and were rejected for the same reasons as claims 1 and 21. Therefore, the arguments presented above apply with equal force to these claims, as well.

Applicants assert that numerous ones of the dependent claims recite further distinctions over the cited art. Applicants traverse the rejections of these claims for at least the reasons given above in regard to the claims from which they depend. However, since the rejections have been shown to be unsupported for the independent claims, a discussion of the dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-31500/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: March 11, 2009